

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yoshihisa ARAI

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: Herewith

FOR: RANDOM NUMBER'S SEED GENERATING CIRCUIT, DRIVER HAVING THE SAME, AND SD
MEMORY CARD SYSTEM

#3
jc997 U.S. PTO
10/09/003
03/06/02

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

APPLICATION NUMBER

MONTH/DAY/YEAR

Japan

2001-063988

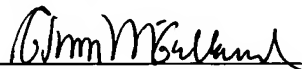
March 7, 2001

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

0181576-1

日 本 国 特 許 庁

JAPAN PATENT OFFICE

1c997 U.S. PTO
10/091003
03/06/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 3月 7日

出 願 番 号

Application Number:

特願2001-063988

出 願 人

Applicant(s):

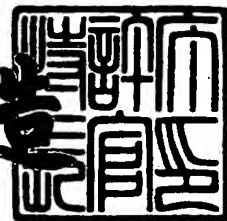
株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年12月14日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願
【整理番号】 A000007586
【提出日】 平成13年 3月 7日
【あて先】 特許庁長官 殿
【国際特許分類】 G11C 7/00
【発明の名称】 乱数シード生成回路及びこれを備えたドライバ、並びに
、SDメモ리카ードシステム
【請求項の数】 18
【発明者】
【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝マ
イクロエレクトロニクスセンター内
【氏名】 新居 欣久
【特許出願人】
【識別番号】 000003078
【氏名又は名称】 株式会社 東芝
【代理人】
【識別番号】 100058479
【弁理士】
【氏名又は名称】 鈴江 武彦
【電話番号】 03-3502-3181
【選任した代理人】
【識別番号】 100084618
【弁理士】
【氏名又は名称】 村松 貞男
【選任した代理人】
【識別番号】 100068814
【弁理士】
【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 乱数シード生成回路及びこれを備えたドライバ、並びに、

SDメモ리카ードシステム

【特許請求の範囲】

【請求項1】 クロックを生成する発振器と、前記クロックに同期して動作するカウンタとを具備し、前記カウンタのカウント値は、前記クロックと非同期の信号にตอบสนองして出力され、その出力された前記カウント値が乱数を作成するための初期値として使用されることを特徴とする乱数シード生成回路。

【請求項2】 クロックを生成する発振器と、前記クロックに同期して動作するカウンタとを具備し、前記カウンタのカウント値を出力するタイミングは、信号にตอบสนองして一定範囲内でランダムに変化し、その出力された前記カウント値が乱数を作成するための初期値として使用されることを特徴とする乱数シード生成回路。

【請求項3】 前記信号は、電源が投入され、電源電位が安定したことを検知したパワーオンリセット回路から出力される信号であることを特徴とする請求項1又は2記載の乱数シード生成回路。

【請求項4】 前記信号は、コントローラから出力される動作開始信号であることを特徴とする請求項1又は2記載の乱数シード生成回路。

【請求項5】 前記動作開始信号は、電源が投入されたことを前記コントローラが認識したときに出力されることを特徴とする請求項4記載の乱数シード生成回路。

【請求項6】 前記動作開始信号は、機器利用者による所定の操作が行われたことを前記コントローラが認識したときに出力されることを特徴とする請求項4記載の乱数シード生成回路。

【請求項7】 前記発振器は、前記信号にตอบสนองして前記カウント値が出力された後に、非動作状態又は前記クロックの周波数を低くした状態となることを特徴とする請求項1又は2記載の乱数シード生成回路。

【請求項8】 前記発振器は、外部端子を持つ電圧制御可能な発振器であり、前記カウント値が出力される前は、前記外部端子と前記発振器が電氣的に切断

され、前記カウント値が出力された後は、前記外部端子と前記発振器が電氣的に接続されることを特徴とする請求項1又は2記載の乱数シード生成回路。

【請求項9】 前記発振器と前記外部端子の間には、前記信号により制御されるスイッチ回路が接続されることを特徴とする請求項8記載の乱数シード生成回路。

【請求項10】 前記カウント値が出力された後は、前記クロックは、システムクロックとして使用されることを特徴とする請求項8記載の乱数シード生成回路。

【請求項11】 前記カウント値を出力するタイミングは、前記カウント値を出力する度に、前記クロックの周期よりも長い時間の範囲内で変化することを特徴とする請求項1又は2記載の乱数シード生成回路。

【請求項12】 前記信号に基づいて前記カウント値をラッチするラッチ回路をさらに具備し、前記ラッチ回路にラッチされた前記カウント値が前記初期値として使用されることを特徴とする請求項1又は2記載の乱数シード生成回路。

【請求項13】 前記信号が入力される乱数生成回路が動作状態となると同時に、前記カウント値が前記初期値として前記乱数生成回路に取り込まれることを特徴とする請求項1又は2記載の乱数シード生成回路。

【請求項14】 クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とを具備し、前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿を行うことを特徴とするドライバ。

【請求項15】 クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とを具備し、前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿を行うことを特徴とするドライバ。

【請求項 16】 前記乱数は、電源が投入される度、前記データの書き込み若しくは読み出しを行う度、又は、機器利用者による所定の操作が行われる度に、作成されることを特徴とする請求項 14 又は 15 記載のドライバ。

【請求項 17】 クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とから構成されるドライバと、

前記ドライバにより駆動されるデータ保護機能を有する SD メモリカードとを具備し、

前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿を行うことを特徴とする SD メモリカードシステム。

【請求項 18】 クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とから構成されるドライバと、

前記ドライバにより駆動されるデータ保護機能を有する SD メモリカードとを具備し、

前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿を行うことを特徴とする SD メモリカードシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、乱数を生成するときの初期値（シード）を決める乱数シード生成回路に関し、特に、デジタル信号処理回路に使用される。

【0002】

【従来の技術】

従来、デジタル信号処理回路などのLSIに乱数生成回路が搭載される場合、この乱数生成回路は、シフトレジスタや演算器などから構成される。乱数を生成する手法としては、従来より多種多様な手法が提案されているが、乱数を生成する元となる初期値（シード）については、システムの特性などを考慮して決めなければならないため、難しい問題の一つとなっている。

【0003】

例えば、乱数生成回路により生成される乱数が適当な周期で変化していればよい（初期値はいつでもよい）システムの場合には、乱数シード（乱数の種）、即ち、初期値が、乱数を生成する度に、同じ値又は高い確率でほぼ同じ値になっても問題はない。このようなシステムとしては、例えば、乱数を用いてホワイトノイズを発生させるデジタルオーディオシステムなどが考えられる。

【0004】

しかし、乱数生成回路により生成される乱数が、適当な周期で変化するだけでなく、その初期値が起動の度に異なる値となることが必要なシステムの場合には、乱数シード、即ち、初期値を、乱数を生成する度に、異なる値に設定しなければならない。このようなシステムとしては、図13に示すように、乱数を用いてセキュリティに関する処理を行うシステム、例えば、SDメモ리카ード（SD memory card）とそのドライバ（プレーヤ）との間で転送データを暗号化して秘匿するシステムが考えられる。

【0005】

【発明が解決しようとする課題】

上述のように、乱数生成回路により生成される乱数が、適当な周期で変化するだけでなく、その初期値が起動の度に異なる値となることが必要なシステムの場合には、乱数シード、即ち、乱数の生成の元となる初期値を、乱数を生成する度に、異なる値に設定しなければならない。

【0006】

しかし、従来の乱数生成回路では、乱数シードを、毎回、異なる値に設定することが非常に難しくなっている。

【0007】

例えば、乱数生成回路がシフトレジスタから構成される場合を考えると、図14に示すように、通常、電源が投入される度（乱数を生成する度）に、パワーオンリセット回路10により、乱数生成回路（シフトレジスタ）11の値がリセットされる。つまり、乱数生成回路11のリセット動作により、その初期値は、常に、同じ値となってしまう。

【0008】

また、このような事態を回避するため、パワーオンリセット回路10により乱数生成回路11の値がリセットされないようにしても、乱数生成回路11の初期値は、チップごとに、高い確率で、同じ値となってしまう。

【0009】

そこで、例えば、図15に示すように、LSIに不揮発性メモリ12を搭載し、電源を切った後には、この不揮発性メモリ12に乱数生成回路（シフトレジスタ）11の値を保持し、かつ、次の電源投入時には、この不揮発性メモリ12に記憶された値を初期値として用いる、という技術がある。

【0010】

しかし、一般的に、LSIに不揮発性メモリを搭載すると、LSIの製造コストが増大する、という問題が発生する。また、LSIによっては、製造プロセス上の理由から、不揮発性メモリを搭載することが非常に困難な場合がある。

【0011】

本発明は、上述の問題を解決するためになされたもので、その目的は、不揮発性メモリを必要とすることなく、かつ、簡易な構成により、乱数シード（乱数生成回路に与える初期値）を起動の度にランダムに異ならせることができる乱数シード生成回路を提案することにある。

【0012】

【課題を解決するための手段】

(1) 本発明の乱数シード生成回路は、クロックを生成する発振器と、前記クロックに同期して動作するカウンタとを備え、前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が乱数を作成するための初期値として使用される。

【0013】

本発明の乱数シード生成回路は、クロックを生成する発振器と、前記クロックに同期して動作するカウンタとを備え、前記カウンタのカウント値を出力するタイミングは、信号に応じて一定範囲内でランダムに変化し、その出力された前記カウント値が乱数を作成するための初期値として使用される。

【0014】

前記信号は、電源が投入され、電源電位が安定したことを検知したパワーオンリセット回路から出力される信号である。

【0015】

前記信号は、コントローラから出力される動作開始信号である。前記動作開始信号は、例えば、電源が投入されたことを前記コントローラが認識したときに出力される信号、又は、機器利用者による所定の操作が行われたことを前記コントローラが認識したときに出力される信号である。

【0016】

前記発振器は、前記信号に応答して前記カウント値が出力された後に、非動作状態又は前記クロックの周波数を低くした状態となる。

【0017】

前記発振器は、外部端子を持つ電圧制御可能な発振器であり、前記カウント値が出力される前は、前記外部端子と前記発振器が電氣的に切断され、前記カウント値が出力された後は、前記外部端子と前記発振器が電氣的に接続される。

【0018】

前記発振器と前記外部端子の間には、前記信号により制御されるスイッチ回路が接続される。

【0019】

前記カウント値が出力された後は、前記クロックは、システムクロックとして使用される。

【0020】

前記カウント値を出力するタイミングは、前記カウント値を出力する度に、前記クロックの周期よりも長い時間の範囲内で変化する。

【0021】

前記信号に基づいて前記カウント値をラッチするラッチ回路をさらに備え、前記ラッチ回路にラッチされた前記カウント値が前記初期値として使用される。

【0022】

前記信号が入力される乱数生成回路が動作状態となると同時に、前記カウント値が前記初期値として前記乱数生成回路に取り込まれる。

【0023】

(2) 本発明のドライバは、クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とを備える。前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿が行われる。

【0024】

本発明のドライバは、クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とを備える。前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿が行われる。

【0025】

前記乱数は、電源が投入される度、前記データの書き込み若しくは読み出しを行う度、又は、機器利用者による所定の操作が行われる度に、作成される。

【0026】

(3) 本発明のSDメモリカードシステムは、クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とから構成されるドライバとを備える。さらに、本発明のSDメモリカードシステムは、前記ドライバにより駆動されるデータ保護機能を有するSDメモリカ

ードを備える。

【0027】

前記カウンタのカウント値は、前記クロックと非同期の信号に応答して出力され、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿が行われる。

【0028】

本発明のSDメモリカードシステムは、クロックを生成する発振器及び前記クロックに同期して動作するカウンタを有する乱数シード生成回路と、前記乱数シード生成回路により生成された初期値を用いて乱数を生成する乱数生成回路とから構成されるドライバとを備える。さらに、本発明のSDメモリカードシステムは、前記ドライバにより駆動されるデータ保護機能を有するSDメモリカードを備える。

【0029】

前記カウンタのカウント値を出力するタイミングは、信号に応答して一定範囲内でランダムに変化し、その出力された前記カウント値が前記初期値として使用され、前記乱数を用いて転送データの秘匿が行われる。

【0030】

【発明の実施の形態】

以下、図面を参照しながら、本発明の乱数シード生成回路について詳細に説明する。

【0031】

本発明の乱数シード生成回路は、不揮発性メモリを用いることなく、かつ、簡易な構成により乱数シードをランダムに生成することができる点に特徴を有する。以下では、まず、乱数シードをランダムに生成するための実施の形態を説明し、その後、本発明の乱数シード生成回路を用いたシステムの一例（応用例）について説明する。

【0032】

〔第1実施の形態〕

図1は、本発明の第1実施の形態に関わる乱数シード生成回路について示して

いる。

【0033】

乱数生成回路11は、乱数シード生成回路13から出力される乱数シード（初期値）に基づいて乱数を生成する。

【0034】

乱数シード生成回路13は、電源投入直後からクロックを生成し始める発振器14と、この発振器14から出力されるクロックに基づいて、カウント値を、順次、増加（又は減少）していくカウンタ15と、取り込み信号に基づいてカウンタ15のカウント値を取り込むラッチ回路16とから構成される。

【0035】

発振器14は、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器14が最も先に動作し始めなければならない。また、発振器14は、周期が数 ns （例えば、 $5ns$ 程度）の高速クロックを生成する。

【0036】

なお、LSI（例えば、デジタル信号処理回路）内に、十分に高い周波数（例えば、 $200MHz$ 程度）のクロックを生成する発振器（例えば、リングオシレータ）が内蔵されている場合には、この発振器により生成したクロックをカウンタ15に与えてもよい。

【0037】

カウンタ15は、このような高速クロックに基づいて動作するため、カウンタ15から出力されるカウント値も高速に変化する。

【0038】

一方、取り込み信号は、発振器14により生成される高速クロックとは非同期であり、かつ、電源が投入されてから取り込み信号がラッチ回路16に入力されるまでの時間は、一定の範囲（例えば、数 μs ～数百 ms ）内で変化しており、この範囲は、発振器14により生成されるクロックの周期（数 ns ）に対して十分に広がっている。

【0039】

つまり、電源が投入されてから取り込み信号がラッチ回路16に入力されるまでの時間は、数 μ s～数百msの範囲でランダムに変化する一方、カウント値は、この範囲内で、数nsの単位で高速に変化しているため、ラッチ回路16にラッチされるカウント値は、電源投入の度に、ランダムに変化することになる。

【0040】

また、ラッチ回路16にラッチされたカウント値は、乱数シード（初期値）となるため、結果として、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【0041】

なお、取り込み信号としては、例えば、パワーオンリセット回路10の出力信号とすることができる。この場合、パワーオンリセット回路10は、電源が投入され、かつ、LSI内部で使用する電源が安定状態となった後に、パワーオンリセット信号（取り込み信号）を出力する。

【0042】

ここで、パワーオンリセット信号は、発振器14により生成されるクロックとは非同期であり、かつ、電源が投入されてからLSI内部で使用する電源が安定状態となるまでの時間は、通常、数 μ s～数百msであるため、パワーオンリセット回路10の出力信号を取り込み信号として用いることは、本発明にとって好都合である。

【0043】

このように、本実施の形態では、例えば、図2の波形図に示すように、電源が投入されてから取り込み信号がラッチ回路16に入力されるまでの時間の範囲を、カウント値が変化する時間（クロックの周期）よりも十分に大きくしており、また、電源が投入されてから取り込み信号がラッチ回路16に入力されるまでの時間は、この範囲内でランダムに変化するため、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【0044】

[第2実施の形態]

本実施の形態に関わる乱数シード生成回路は、上述の第1実施の形態に関わる乱数シード生成回路の変形例である。

【0045】

本実施の形態の乱数シード生成回路は、上述の第1実施の形態に関わる乱数シード生成回路と比べると、① カウント値をラッチするラッチ回路を省略し、② パワーオンリセット回路の出力信号を、乱数生成回路の動作開始信号として、直接、乱数生成回路に入力した点に特徴を有する。

【0046】

この場合、パワーオンリセット回路の出力信号（動作開始信号）は、従来のように、乱数シード（初期値）をリセットしない。即ち、本実施の形態では、パワーオンリセット回路の出力信号が乱数生成回路に入力された時点で、乱数シード生成回路内のカウンタのカウント値に基づいて乱数シードが決定され、かつ、乱数生成回路において乱数を生成する動作が開始する。

【0047】

以下、本実施の形態に関わる乱数シード生成回路について詳細に説明する。

【0048】

図3は、本発明の第2実施の形態に関わる乱数シード生成回路について示している。

【0049】

乱数生成回路11は、乱数シード生成回路13から出力される乱数シード（初期値）に基づいて乱数を生成する。乱数シード生成回路13は、電源投入直後からクロックを生成し始める発振器14と、この発振器14から出力されるクロックに基づいて、カウント値を、順次、増加（又は減少）していくカウンタ15とから構成される。

【0050】

発振器14は、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器14が最も先に動作し始めなければならない。また、発振器14は、周期が数ns（

例えば、5 ns 程度) の高速クロックを生成する。

【0051】

なお、上述の第1実施の形態と同様に、LSI内に設けられる別の発振器(例えば、リングオシレータ)を利用して、カウンタ15に与えるクロックを生成してもよい。

【0052】

カウンタ15は、このような高速クロックに基づいて動作するため、カウンタ15から出力されるカウント値も高速に変化する。

【0053】

一方、動作開始信号は、発振器14により生成される高速クロックとは非同期であり、かつ、電源が投入されてからLSI内部で使用する電源が安定状態となるまでの時間、具体的には、電源が投入された後、パワーオンリセット回路10から動作開始信号が出力されるまでの時間は、一定の範囲(例えば、数 μ s~数百ms)内で変化しており、この範囲は、発振器14により生成されるクロックの周期(数ns)に対して十分に広がっている。

【0054】

つまり、電源が投入されてから動作開始信号が乱数生成回路11に入力されるまでの時間は、数 μ s~数百msの範囲でランダムに変化する一方、カウント値は、この範囲内で、数nsの単位で高速に変化しているため、乱数生成回路11が動作を開始するときの乱数シード(カウント値)は、電源投入の度に、ランダムに変化する。

【0055】

このように、本実施の形態では、電源が投入されてから、動作開始信号が乱数生成回路11に入力されるまでの時間の範囲を、カウント値が変化する時間(クロックの周期)よりも十分に大きくしている。このため、電源が投入されてから動作開始信号が乱数生成回路11に入力されるまでの時間が、この範囲内でランダムに変化することにより、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【0056】

また、本実施の形態では、カウンタ15のカウント値が、直接、乱数生成回路11に入力される。そして、動作開始信号が乱数生成回路に入力された時点で、乱数シードが決定され、同時に、乱数生成回路において乱数を生成する動作が開始される。このため、乱数シード生成回路の面積縮小、設計容易化、製造コストの低下などの独自の効果を得ることができる。

【0057】

〔第3実施の形態〕

図4は、本発明の第3実施の形態に関わる乱数シード生成回路について示している。

【0058】

乱数生成回路11は、乱数シード生成回路13から出力される乱数シード（初期値）に基づいて乱数を生成する。

【0059】

乱数シード生成回路13は、電源投入直後からクロックを生成し始める発振器14と、この発振器14から出力されるクロックに基づいて、カウント値を、順次、増加（又は減少）していくカウンタ15と、コントローラ21からの動作開始信号（取り込み信号）に基づいてカウンタ15のカウント値を取り込むラッチ回路16とから構成される。

【0060】

発振器14は、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器14が最も先に動作し始めなければならない。また、発振器14は、周期が数 ns （例えば、 $5ns$ 程度）の高速クロックを生成する。

【0061】

なお、上述の第1実施の形態と同様に、LSI内に設けられる別の発振器（例えば、リングオシレータ）を利用して、カウンタ15に与えるクロックを生成してもよい。

【0062】

カウンタ15は、このような高速クロックに基づいて動作するため、カウンタ15から出力されるカウント値も高速に変化する。

【0063】

一方、カウンタ15のカウント値をラッチ回路16に取り込むタイミングは、コントローラ（ホストマイコン）21からの動作開始信号により決定される。

【0064】

コントローラ21からの動作開始信号とは、何らかの処理を行うために乱数が必要になったときに、コントローラ21が乱数生成回路11を動作させるために出力する信号のことであり、発振器14により生成されるクロックとは非同期である。

【0065】

例えば、SDカードを使ったシステム（図12）では、システムコントロール用CPU（コントローラ）21、SDカードインターフェイス回路22や、その他のデジタル信号処理回路（DSP）23などを用いて、SDカード24にデータを書き込んだり、又は、SDカード24からデータを読み出したりする。

【0066】

ここで、SDカード24に対してデータの書き込み又は読み出しを行う際には、システムコントロール用CPU21は、SDカード24へのアクセスを指示する信号を出力することになる。

【0067】

そこで、このSDカード24に対するアクセスを指示する信号を、動作開始信号としてラッチ回路16に供給し、乱数シードの取り込みに利用する。

【0068】

一般に、システムコントロール用CPU21の動作クロックは、SDカードインターフェイス回路22の動作を制御するクロックに対して非同期であり、さらに、システムコントロール用CPU21から出力される動作開始信号の周期は、数 μ s程度となっている。つまり、カウンタ15の動作速度（カウント値が変化する速度）は、この動作開始信号の動作速度（周波数）よりも十分に速くなっているため、ラッチ回路16にラッチされるカウント値は、動作開始信号が出力さ

れる度に、ランダムに変化することになる。

【0069】

また、ラッチ回路16にラッチされたカウント値は、乱数シード（初期値）となるため、結果として、乱数シードを、動作開始信号が出力される度に、ランダムに変化させることができる。

【0070】

このように、本実施の形態では、システムコントローラ21からの動作開始信号に基づいて、カウント値を取り込むタイミング、即ち、乱数シードを決定している。従って、乱数シードを、動作開始信号を出力する度に、ランダムに変化させることができる。

【0071】

なお、本実施の形態においては、システムコントローラ21からの動作開始信号を、機器利用者（又はシステム利用者）の操作によるタイミングとすることが可能である。例えば、SDカードを使ったオーディオプレーヤであれば、機器利用者が再生ボタンを押したタイミングや、SDカードをプレーヤ内に挿入したタイミングで、動作開始信号が出力されるようにしてもよい。

【0072】

〔第4実施の形態〕

本実施の形態に関わる乱数シード生成回路は、上述の第3実施の形態に関わる乱数シード生成回路の変形例である。

【0073】

本実施の形態の乱数シード生成回路は、上述の第3実施の形態の乱数シード生成回路と比べると、① カウント値をラッチするラッチ回路を省略し、② コントローラ21からの動作開始信号を、直接、乱数生成回路に入力した点に特徴を有する。

【0074】

この場合、コントローラ21からの動作開始信号が乱数生成回路に入力された時点で、乱数シード生成回路内のカウンタのカウント値に基づいて乱数シードが決定され、かつ、乱数生成回路において乱数を生成する動作が開始する。

【0075】

以下、本実施の形態に関わる乱数シード生成回路について詳細に説明する。

【0076】

図5は、本発明の第4実施の形態に関わる乱数シード生成回路について示している。

【0077】

乱数生成回路11は、乱数シード生成回路13から出力される乱数シード（初期値）に基づいて乱数を生成する。乱数シード生成回路13は、電源投入直後からクロックを生成し始める発振器14と、この発振器14から出力されるクロックに基づいて、カウント値を、順次、増加（又は減少）していくカウンタ15とから構成される。

【0078】

発振器14は、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器14が最も先に動作し始めなければならない。また、発振器14は、周期が数ns（例えば、5ns程度）の高速クロックを生成する。

【0079】

なお、上述の第1実施の形態と同様に、LSI内に設けられる別の発振器（例えば、リングオシレータ）を利用して、カウンタ15に与えるクロックを生成してもよい。

【0080】

カウンタ15は、このような高速クロックに基づいて動作するため、カウンタ15から出力されるカウント値も高速に変化する。

【0081】

一方、カウンタ15のカウント値が乱数シードとして乱数生成回路11に入力されるタイミングは、コントローラ（ホストマイコン）21からの動作開始信号により決定される。

【0082】

コントローラ 21 からの動作開始信号とは、何らかの処理を行うために乱数が必要になったときに、コントローラ 21 が乱数生成回路 11 を動作させるために出力する信号のことであり、発振器 14 により生成されるクロックとは非同期である。

【0083】

なお、コントローラ 21 から動作開始信号が出力されるタイミングとしては、機器利用者（又はシステム利用者）の操作によるタイミングを利用することができる。例えば、SD カードを使ったオーディオプレーヤであれば、システム利用者が再生ボタンを押したタイミングや、SD カードをシステム内に挿入したタイミングで、動作開始信号が出力されるようにしてもよい。

【0084】

このように、本実施の形態では、コントローラ 21 からの動作開始信号に基づいて、カウント値を取り込むタイミング、即ち、乱数シードを決定している。従って、乱数シードを、動作開始信号を出力する度に、ランダムに変化させることができる。

【0085】

また、本実施の形態では、カウンタ 15 のカウント値が、直接、乱数生成回路 11 に入力され、動作開始信号に基づいて乱数シードが決定される。このため、乱数シード生成回路の面積縮小、設計容易化、製造コストの低下などの独自の効果を得ることができる。

【0086】

〔第 5 実施の形態〕

本実施の形態に関わる乱数シード生成回路は、上述の第 3 実施の形態に関わる乱数シード生成回路の変形例である。

【0087】

図 6 は、本発明の第 5 実施の形態に関わる乱数シード生成回路について示している。

【0088】

本実施の形態の乱数シード生成回路 13 は、上述の第 3 実施の形態の乱数シード

ド生成回路と比べると、コントローラ 2 1 からの動作開始信号を、発振器 1 4 の動作を停止させる発振停止信号として、発振器 1 4 にも入力した点に特徴を有する。その他の構成については、上述の第 3 実施の形態に関わる乱数シード生成回路と全く同一である。

【 0 0 8 9 】

本発明の乱数シード生成回路 1 3 では、乱数シード（初期値）が決定された後には、乱数シード生成回路 1 3 を動作させておく必要がない。

【 0 0 9 0 】

そこで、本実施の形態では、コントローラ 2 1 からの動作開始信号により、乱数シードをラッチ回路 1 6 にラッチすると同時に、発振器 1 4 の動作を停止させて、消費電力の削減を図っている。

【 0 0 9 1 】

なお、本実施の形態では、乱数シードが決定された後に、発振器 1 4 を非動作状態にしたが、例えば、これに代えて、発振器 1 4 により生成されるクロックの周波数を十分に低くしても、消費電力の削減を実現できる。

【 0 0 9 2 】

〔第 6 実施の形態〕

本実施の形態に関わる乱数シード生成回路は、上述の第 4 実施の形態に関わる乱数シード生成回路の変形例である。

【 0 0 9 3 】

図 7 は、本発明の第 6 実施の形態に関わる乱数シード生成回路について示している。

【 0 0 9 4 】

本実施の形態の乱数シード生成回路 1 3 は、上述の第 4 実施の形態の乱数シード生成回路と比べると、コントローラ 2 1 からの動作開始信号を、発振器 1 4 の動作を停止させる発振停止信号として、発振器 1 4 にも入力した点に特徴を有する。その他の構成については、上述の第 4 実施の形態に関わる乱数シード生成回路と全く同一である。

【 0 0 9 5 】

上述の第5実施の形態で説明したように、本発明の乱数シード生成回路では、コントローラ21からの動作開始信号により、乱数シード（初期値）が決定された後には、乱数シード生成回路13を動作させておく必要がない。

【0096】

そこで、本実施の形態では、コントローラ21からの動作開始信号により、乱数生成回路11が動作し、乱数シードが決定されると同時に、発振器14の動作を停止させて、消費電力の削減を図っている。

【0097】

なお、本実施の形態においても、発振器14に関しては、乱数生成回路11を動作状態にした後には、発振周波数を十分に低くして、消費電力の削減を図ってもよい。

【0098】

【第7実施の形態】

本実施の形態に関わる乱数シード生成回路は、悪意を持って本発明の集積回路を解析する、という行為を防止すべく、電源が投入されてから乱数シードの取り込みが完了するまでは、LSIの外部から乱数シード生成回路内の発振器を制御できないようにした点、及び、乱数シード生成回路内の発振器から出力されるクロックを、乱数を用いて動作するシステムの動作クロックとして使用した点に特徴を有する。

【0099】

図8は、本発明の第7実施の形態に関わる乱数シード生成回路について示している。

【0100】

乱数生成回路11は、乱数シード生成回路13から出力される乱数シード（初期値）に基づいて乱数を生成する。

【0101】

乱数シード生成回路13は、電源投入直後からクロックを生成し始める電圧制御可能な発振器（VCO：Voltage Controlled Oscillator）14Aと、この発振器14Aから出力されるクロックに基づいて、カウント値を、順次、増加（

又は減少) していくカウンタ15と、コントローラ21からの動作開始信号(取り込み信号)に基づいてカウンタ15のカウント値を取り込むラッチ回路16とを有する。

【0102】

また、本実施の形態では、発振器14Aから出力されるクロックをシステム動作クロックとしても使用している。このため、乱数シード生成回路13は、さらに、発振器14Aから出力されるクロックの周波数を一定値に安定させるためのPLL(Phase Locked Loop)回路を備えている。

【0103】

PLL回路は、基準クロックの周波数を分周する分周器17Aと、発振器14Aから出力されるクロックを分周する分周器17Bと、分周器17Aから出力されるクロックと分周器17Bから出力されるクロックの位相を比較する位相比較器18と、抵抗及びキャパシタからなるLPF(ローパスフィルタ)19と、コントローラ21からの動作開始信号により制御されるスイッチ回路24とから構成される。

【0104】

発振器14Aは、電源が投入されると直ちに自己発振し、各機能ブロックや各回路などに発振出力を供給しなければならない。各機能ブロックや各回路などを動作可能状態にするためである。言い換えれば、電源が投入されると、発振器14Aが最も先に動作し始めなければならない。

【0105】

また、発振器14Aは、周期が数ns(例えば、5ns程度)の高速クロックを生成する。この時、スイッチ回路24は、オフ状態となっており、PLL回路は、機能していない。LSIの外部から発振器14Aの周波数を制御できないようにするためである。

【0106】

なお、カウンタ15は、このような高速クロックに基づいて動作するため、カウンタ15から出力されるカウント値も高速に変化する。

【0107】

一方、電源が投入されてから数 μ s～数百msが経過した後に、コントローラ21からの動作開始信号がラッチ回路16及びスイッチ回路24に入力される。この範囲は、発振器14Aにより生成されるクロックの周期（数ns）に対して十分に広くなっており、また、動作開始信号は、発振器14により生成されるクロックとは非同期である。

【0108】

つまり、電源が投入されてからコントローラ21からの動作開始信号がラッチ回路16に入力されるまでの時間は、数 μ s～数百msの範囲でランダムに変化する一方、カウント値は、この範囲内で、数nsの単位で高速に変化するため、ラッチ回路16にラッチされるカウント値は、電源投入の度に、ランダムに変化することになる。

【0109】

また、ラッチ回路16にラッチされたカウント値は、乱数シード（初期値）となるため、結果として、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【0110】

ところで、本実施の形態では、コントローラ21からの動作開始信号がラッチ回路16に入力され、乱数シードが決定されると同時に、スイッチ回路24がオン状態となり、PLL回路が機能し始める。そして、乱数シード生成回路13内の発振器14Aから出力されるクロックを、乱数を用いて動作するシステムの動作クロックとしても使用する。

【0111】

例えば、図12に示すようなシステムにおいては、インターフェイス回路22を動作させるために、20メガHz程度の動作クロックが必要となるが、この動作クロックとして、図8の乱数シード生成回路13内の発振器14Aから出力されるクロックを使用する。

【0112】

通常のLSIでは、多くの場合、発振器（VCO）から出力されるクロックの周波数を一定値に安定させるためには、PLL回路による制御が必要となる。こ

ここで、PLL回路は、LPF（ローパスフィルタ）19を備えているが、このLPF19は、LSIの外部に、いわゆる外付け部品として接続される。

【0113】

しかし、このことは、発振器（VCO）から出力されるクロックの周波数（発振周波数）を、LSIの外部から制御できることを意味するため、乱数シードが自由にコントロールされ、悪意の解析者からデータを保護することができなくなる、という問題が生じる。

【0114】

即ち、外付け部品を取り除き、発振器（VCO）14Aを制御する電圧を自由に制御できるようにすれば、例えば、発振器14Aの発振周波数を十分に低くして（カウンタ15のカウント値がほとんど変わらないようにして）、電源投入の度に、乱数シードをほぼ同じ値又は全く同じ値にすることも可能である。

【0115】

そこで、本実施の形態では、電源が投入されてから乱数シードが決定されるまでは、スイッチ回路24をオフ状態にし、発振器（VCO）14AがPLL回路（又はLSI外部の悪意の解析者）により制御されないようにしている。

【0116】

なお、コントローラ21からの動作開始信号により、カウンタ値がラッチ回路16に取り込まれ、かつ、乱数シードが決定された後には、スイッチ回路24がオン状態となり、PLL回路による発振器（VCO）14Aの制御が開始される。

【0117】

スイッチ回路24がオン状態になると、例えば、LSIの外部からの制御により、発振器14Aの発振周波数を極端に低く又は停止させることも可能になるが、本実施の形態では、発振器14Aから出力されるクロックをシステムの動作クロックとしても使用しているため、LSIの動作を解析される恐れはない。

【0118】

つまり、発振器14Aの発振周波数を極端に低く又は停止させると、システム自体が動作しなくなる。

【0119】

このように、本実施の形態では、第一に、電源が投入されてからコントローラ 21 からの動作開始信号（取り込み信号）がラッチ回路 16 に入力されるまでの時間の範囲を、カウント値が変化する時間（クロックの周期）よりも十分に大きくしており、また、電源が投入されてからこの動作開始信号がラッチ回路 16 に入力されるまでの時間は、この範囲内でランダムに変化するため、乱数シードを、電源投入の度に、ランダムに変化させることができる。

【0120】

また、第二に、乱数シード生成回路内の発振器から出力されるクロックを、乱数を用いて動作するシステムの動作クロックとして使用し、かつ、PLL 回路により動作クロックの周波数の安定化を図った場合において、電源が投入されてから乱数シードの取り込みが完了するまでは、LSI の外部から乱数シード生成回路内の発振器を制御できないようにしているため、悪意を持った解析者からデータを保護することができる。

【0121】

[第 8 実施の形態]

図 9 は、本発明の第 8 実施の形態に関わる乱数シード生成回路について示している。

【0122】

本実施の形態に関わる乱数シード生成回路は、上述の第 7 実施の形態に関わる乱数シード生成回路の変形例である。

【0123】

本実施の形態の乱数シード生成回路は、上述の第 7 実施の形態に関わる乱数シード生成回路と比べると、① カウント値をラッチするラッチ回路を省略し、② コントローラ 21 からの動作開始信号を、乱数生成回路 11 の動作開始信号として、直接、乱数生成回路 11 に入力した点に特徴を有する。

【0124】

この場合、コントローラ 21 からの動作開始信号が乱数生成回路 11 に入力された時点で、乱数シード生成回路 13 内のカウンタ 15 のカウント値に基づいて

乱数シードが決定され、かつ、乱数生成回路11において乱数を生成する動作が開始する。

【0125】

このように、本実施の形態では、コントローラ21からの動作開始信号に基づいて、カウント値を取り込むタイミング、即ち、乱数シードを決定している。従って、乱数シードを、動作開始信号を出力する度に、ランダムに変化させることができる。

【0126】

また、乱数シード生成回路内の発振器から出力されるクロックを、乱数を用いて動作するシステムの動作クロックとして使用し、電源が投入されてから乱数シードの取り込みが完了するまでは、LSIの外部から乱数シード生成回路内の発振器を制御できないようにしているため、悪意を持った解析者からデータを保護できる。

【0127】

さらに、本実施の形態では、カウンタ15のカウント値が、直接、乱数生成回路11に入力され、動作開始信号に基づいて乱数シードが決定される。このため、乱数シード生成回路の面積縮小、設計容易化、製造コストの低下などの独自の効果を得ることができる。

【0128】

【応用例】

以下、上述の第1乃至第8実施の形態に関わる乱数シード生成回路を、SDメモ리카ード（Secure Digital Memory Card）を使ったシステムに適用した応用例について説明する。

【0129】

図10及び図11は、SDメモ리카ードシステムの概要を示している。

【0130】

SDメモ리카ードとは、強力な著作権保護機能を有する点を一つの特徴とするメモ리카ードのことである。

【0131】

SDメモ리카ード24内のメモリ領域は、普通にアクセスできるユーザデータエリアと、ドライバ（プレーヤ）20とカード24の間で相互認証が認められた場合にのみアクセスできるプロテクトエリアとから構成される。

【0132】

例えば、SDメモ리카ードに音楽データを書き込む場合、図10に示すように、まず、相互認証が行われる。相互認証が成功した場合には、例えば、コントローラから動作開始信号が出力され、本発明に関わる乱数シード生成回路により乱数シードが生成される。また、この乱数シードを用いて乱数が生成され、プロテクトエリアにアクセスするためのテンポラリーの鍵（セッション鍵）A1が作成される。

【0133】

音楽データは、ドライバ（プレーヤ）20内で鍵Bにより暗号化され、暗号化された音楽データがSDメモ리카ード24内のユーザデータエリアに保存される。また、鍵Bは、SDメモ리카ード24内のプロテクトエリアに保存される。ここで鍵Bは、音楽データを暗号化するために使用したものであり、これが漏洩すると、音楽データの不正なコピーを発生させる危険性がある。

【0134】

そこで、ドライバ20側においては、乱数を使って生成された鍵A1を用いて、セキュリティ部にて鍵Bを暗号化し、これを、SDメモ리카ード24に転送する。これにより、ホストマイコンとSDメモ리카ードの間のバス情報の解析が行われないようにしている。

【0135】

なお、鍵A1は、テンポラリーの鍵であり、プロテクトエリアにアクセスする度（又は電源投入の度）に、本発明に関わる乱数を使って作成され、かつ、プロテクトエリアにアクセスする度（又は電源投入の度）に、異なるものとなる。

【0136】

また、SDメモ리카ードから音楽データを読み出す場合には、図11に示すように、まず、相互認証が行われる。相互認証が成功した場合には、例えば、コントローラから動作開始信号が出力され、本発明に関わる乱数シード生成回路によ

り乱数シードが生成される。また、この乱数シードを用いて乱数が生成され、プロテクトエリアにアクセスするためのテンポラリーの鍵（セッション鍵）A2が作成される。

【0137】

暗号化された音楽データは、SDメモ리카ード24のユーザデータエリアから読み出され、鍵Bは、SDメモ리카ード24のプロテクトエリアから読み出される。ここで、SDメモ리카ード24側においては、鍵Bを読み出すに当たって、乱数を使って生成された鍵A2を用いて、セキュリティ部で鍵Bを暗号化し、これを、ホストマイコンに転送する。これにより、ホストマイコンとSDメモ리카ードの間のバス情報の解析が行われないようにしている。

【0138】

鍵Bは、SDメモ리카ード24側において、鍵A2により復号される。また、この鍵Bを用いて、暗号化された音楽データが復号される。その結果、音楽データが再生される。

【0139】

なお、鍵A2も、テンポラリーの鍵であり、当然に、プロテクトエリアにアクセスする度（又は電源投入の度）に、本発明に関わる乱数を使って生成され、かつ、プロテクトエリアにアクセスする度（又は電源投入の度）に、異なるものとなる。

【0140】

ところで、SDメモ리카ード24から音楽データを読み出す場合において、相互認証が失敗したときには、例えば、コントローラ（ホストマイコン）は、動作開始信号を出力しないため、本発明に関わる乱数は生成させず、結果として、テンポラリーの鍵（セッション鍵）A2も、作成されない。

【0141】

従って、この場合、暗号化された音楽データについては読み出すことができるが、鍵Bを読み出すことができないため、結局、音楽データを再生することができず、音楽データの不正な読み出し又は不正なコピーが防止される。

【0142】

図12は、本発明の乱数シード生成回路を有するドライバとSDメモ리카ードからなるシステムの具体例を示している。

【0143】

23は、デジタル信号処理回路(DSP)であり、乱数生成回路11と、本発明に関わる乱数シード生成回路13とを有している。乱数シード生成回路13は、上述の第1乃至第8実施の形態に関わる乱数シード生成回路のいずれか1つに相当する。

【0144】

インターフェイス回路22は、SDメモ리카ード24とデータのやりとりを行うための回路である。インターフェイス回路22は、例えば、20メガHz程度の動作クロックで制御される。この動作クロックは、例えば、上述の第7及び第8実施の形態に関わる乱数シード生成回路を採用する場合、乱数シード生成回路内の発振器で生成される。

【0145】

パワーオンリセット回路10は、LSIで使用する電源電位が安定した後に、リセット信号を出力する。このリセット信号は、コントローラ(ホストマイコン)21に供給されると共に、上述の第1及び第2実施の形態に関わる乱数シード生成回路の場合には、デジタル信号処理回路23にも供給される。

【0146】

また、上述の第3乃至第6実施の形態に関わる乱数シード生成回路の場合には、コントローラ21は、パワーオンリセット回路10からリセット信号を受けたときに、乱数シード生成回路13に対して動作開始信号を出力する。また、コントローラ21は、機器利用者の操作タイミング(例えば、再生ボタンを押したタイミングや、SDメモ리카ードをドライバに挿入したタイミングなど)に合わせて、動作開始信号を出力してもよい。

【0147】

なお、このシステムにおいて、例えば、インターフェイス回路22とデジタル信号処理回路23は、1チップ内に形成される。また、コントローラ(CPU)21、インターフェイス回路22及びデジタル信号処理回路23を、1チップ化

しても構わない。

【0148】

【発明の効果】

以上、説明したように、本発明の乱数シード生成回路によれば、次のような効果を奏することができる。

【0149】

① 不揮発性メモリを必要とすることなく、高速クロックを発生する発振器とこれよりも遅い取り込み信号（動作開始信号）とを用いることにより、電源投入の度に、乱数シードをランダムに変えることができる。

【0150】

② 取り込み信号としては、パワーオンリセット回路の出力信号又はコントローラからの動作開始信号を用いることができ、簡易な構成により、乱数シードをランダムに変えることができる。

【0151】

③ 機器利用者の操作タイミングを利用して、乱数シード生成回路を動作させることにより、電源投入の度に、乱数シードを確実に変えることができる。

【0152】

④ 乱数シード生成回路により乱数シードを決定した後は、発振器を停止状態にすることにより、LSIの消費電力を小さくすることができる。

【0153】

⑤ 乱数シード生成回路内の発振器をVCOとし、その出力クロックをシステムの動作クロックとして使用する場合に、電源を投入してから乱数シードが決定されるまでは、LSI外部からこの発振器を制御できないようにすることで、悪意をもってLSIの動作を解析することを防止できる。

【図面の簡単な説明】

【図1】

本発明の第1実施の形態に関わる乱数シード生成回路を示す図。

【図2】

図1の乱数シード生成回路の動作を示す波形図。

【図 3】

本発明の第 2 実施の形態に関わる乱数シード生成回路を示す図。

【図 4】

本発明の第 3 実施の形態に関わる乱数シード生成回路を示す図。

【図 5】

本発明の第 4 実施の形態に関わる乱数シード生成回路を示す図。

【図 6】

本発明の第 5 実施の形態に関わる乱数シード生成回路を示す図。

【図 7】

本発明の第 6 実施の形態に関わる乱数シード生成回路を示す図。

【図 8】

本発明の第 7 実施の形態に関わる乱数シード生成回路を示す図。

【図 9】

本発明の第 8 実施の形態に関わる乱数シード生成回路を示す図。

【図 1 0】

SD メモリカードを使用したシステムの概要を示す図。

【図 1 1】

SD メモリカードを使用したシステムの概要を示す図。

【図 1 2】

SD メモリカードとそのドライバからなるシステムを示す図。

【図 1 3】

従来の乱数生成回路の一例を示す図。

【図 1 4】

従来の乱数生成回路の一例を示す図。

【図 1 5】

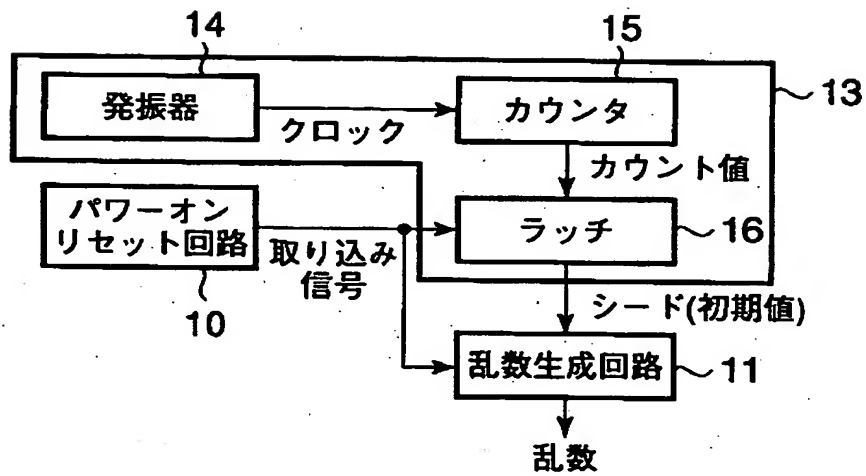
従来の乱数を使用したシステムの一例を示す図。

【符号の説明】

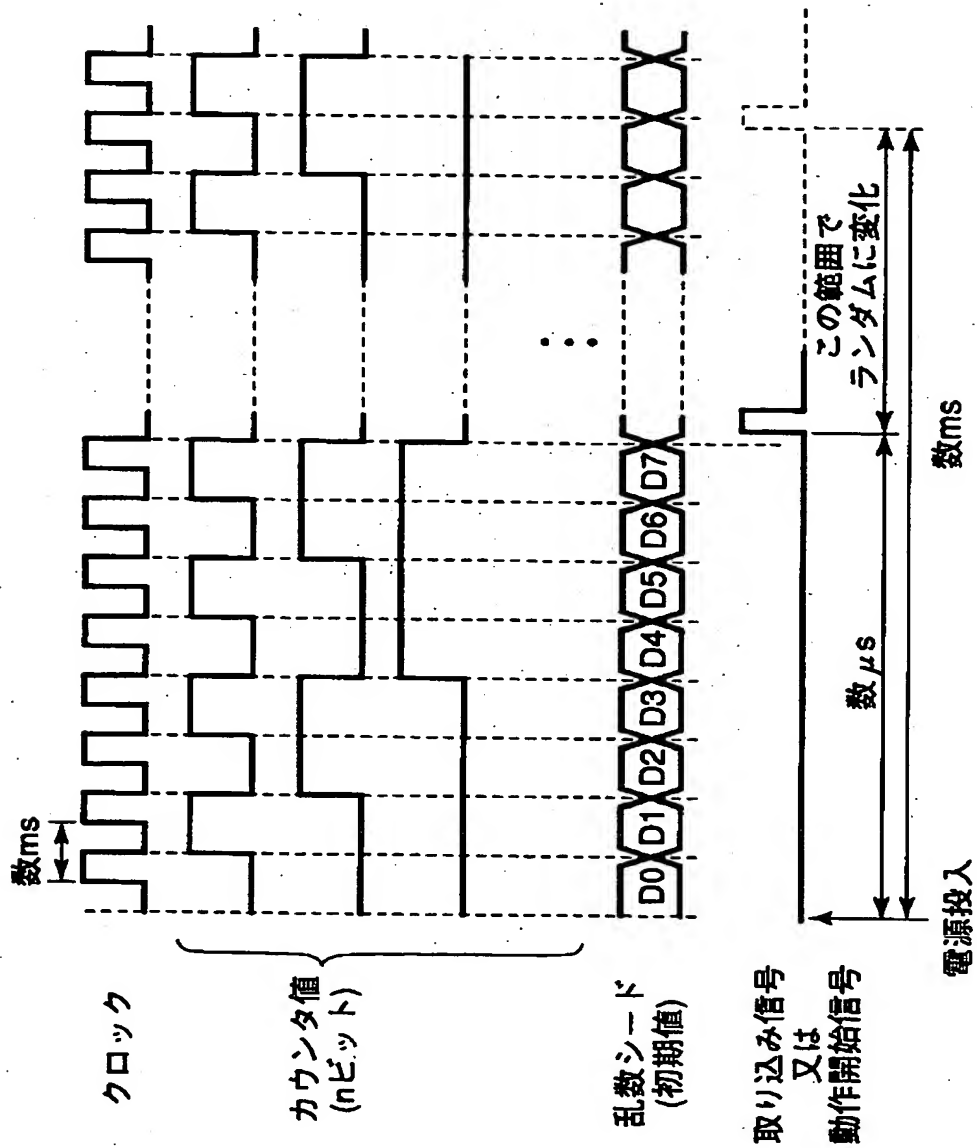
- 1 1 : 乱数生成回路、
- 1 2 : 不揮発性メモリ、

- 13 : 乱数シード生成回路、
- 14 : 発振器、
- 14 A : 電圧制御可能な発振器 (VCO)、
- 15 : カウンタ、
- 16 : ラッチ回路、
- 17 A, 17 B : 分周器、
- 18 : 位相比較器、
- 19 : ローパスフィルタ (LPF)、
- 20 : ドライバ (プレーヤ)、
- 21 : コントローラ、
- 22 : インターフェイス回路、
- 23 : デジタル信号処理回路、
- 24 : スイッチ回路。

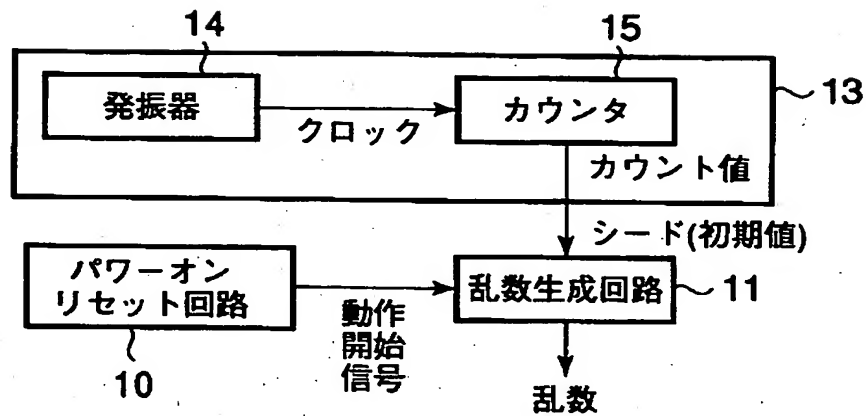
【書類名】 図面
【図1】



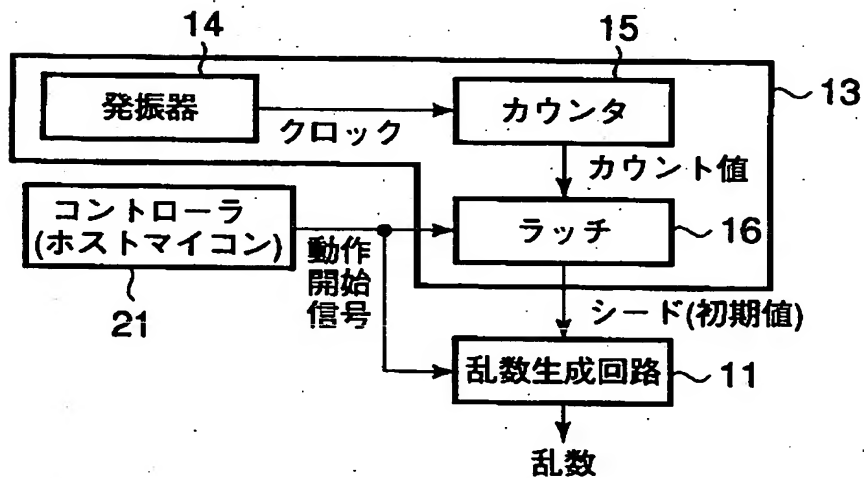
【図2】



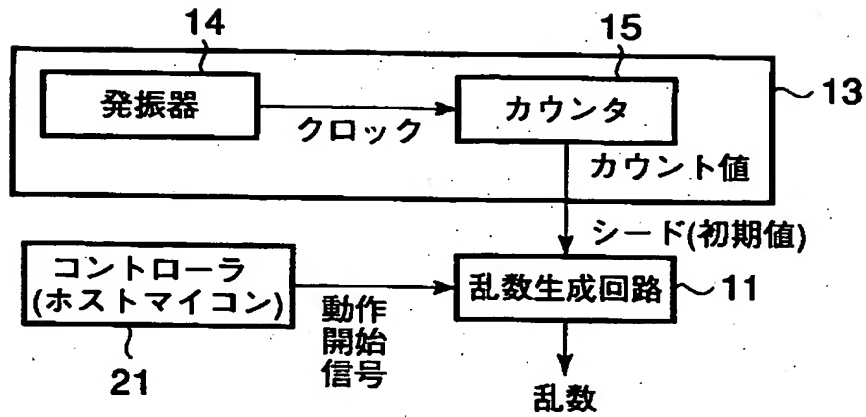
【図3】



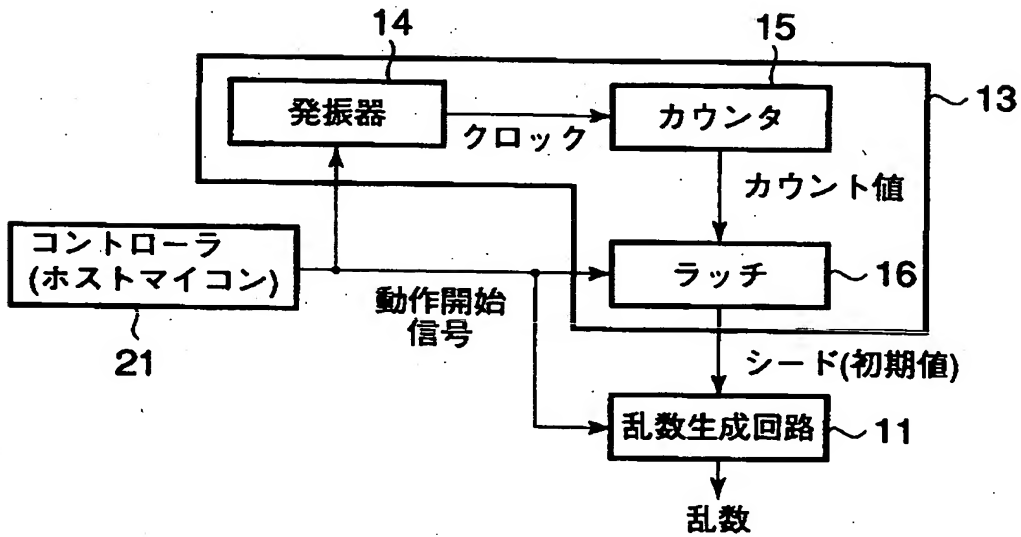
【図4】



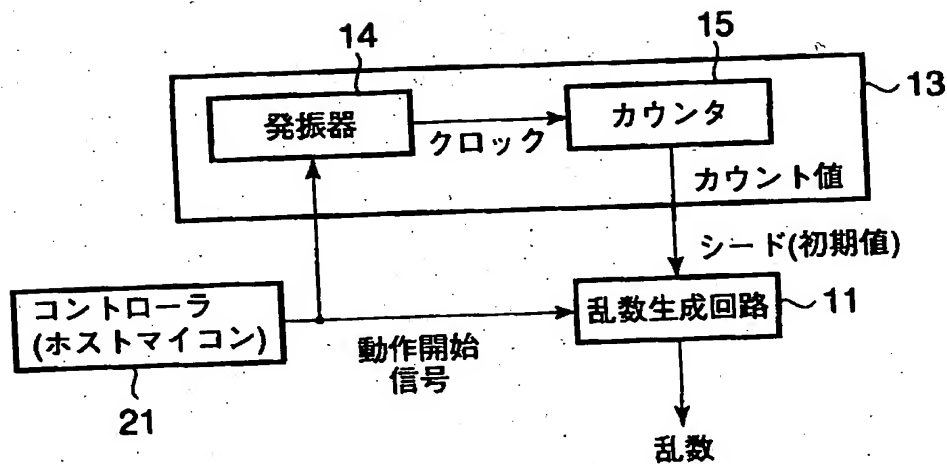
【図 5】



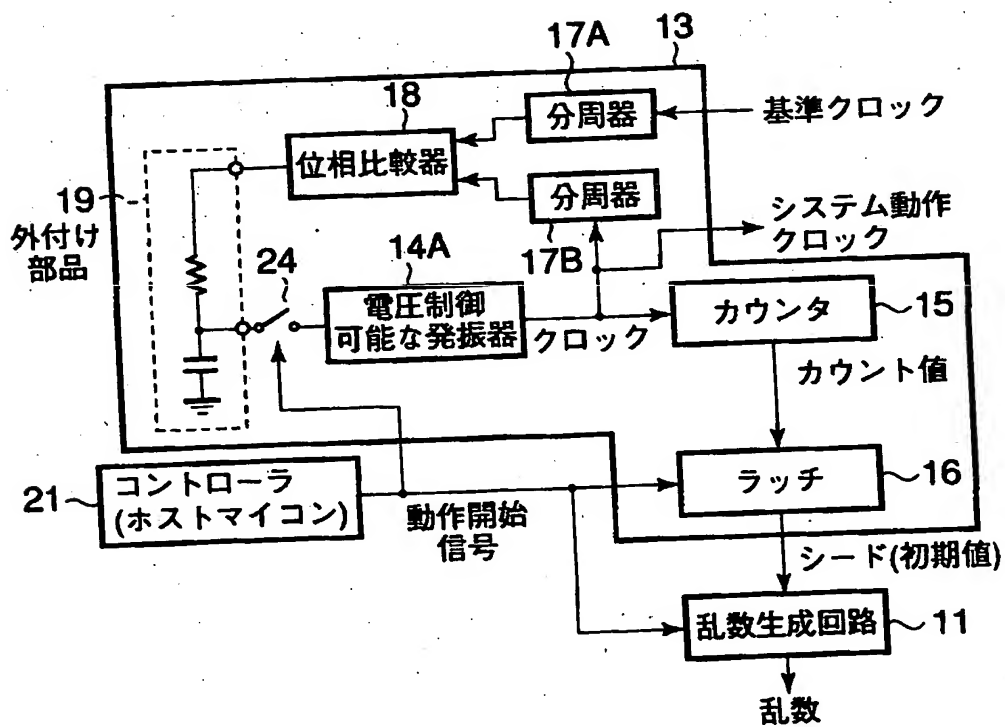
【図 6】



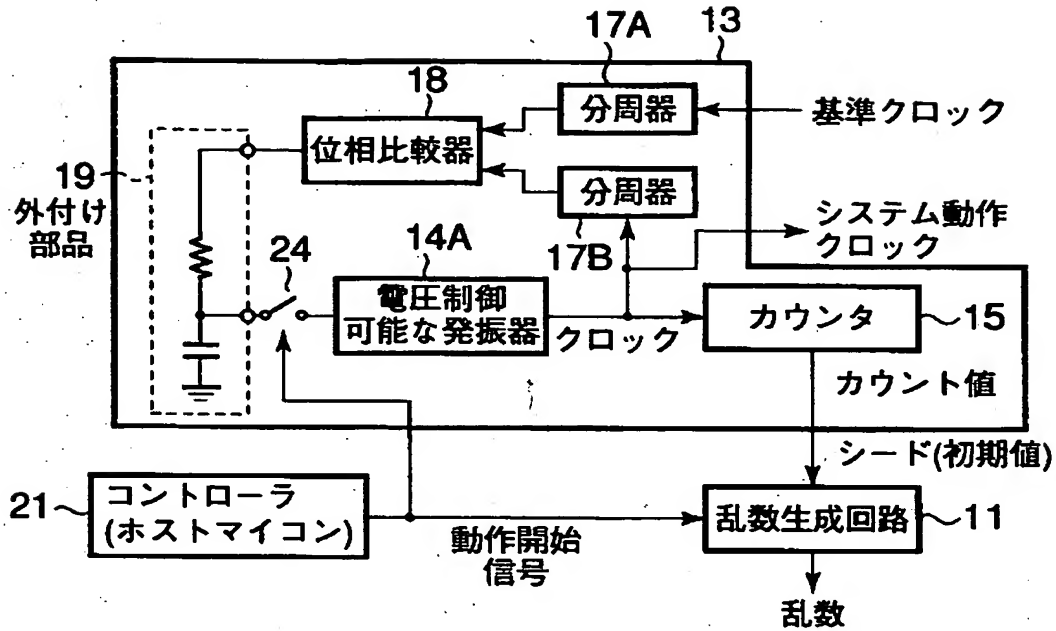
【図7】



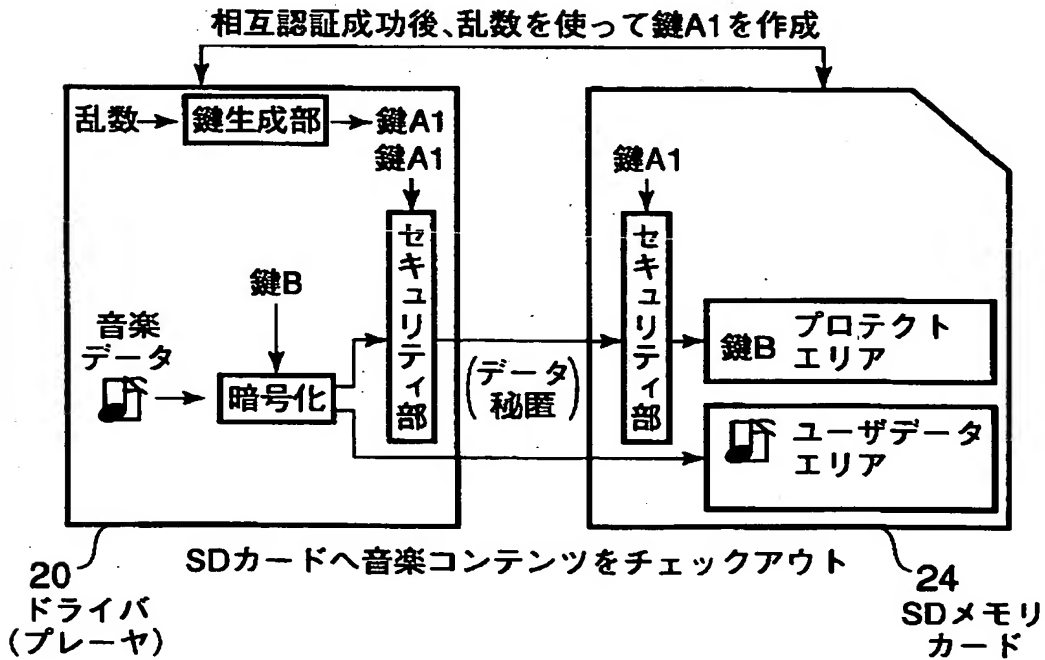
【図8】



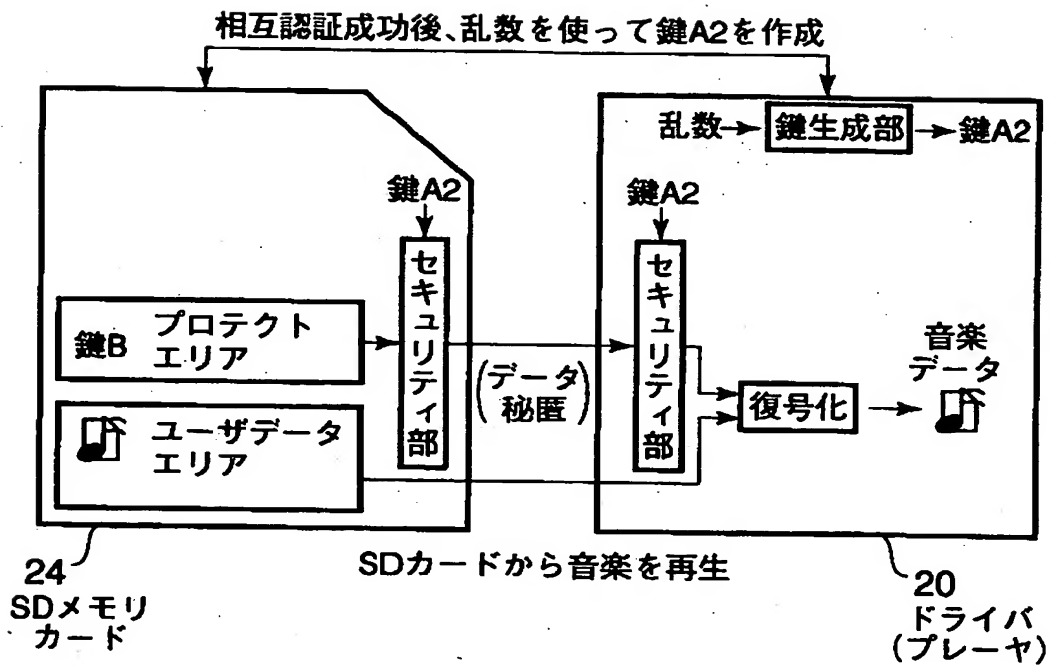
【図9】



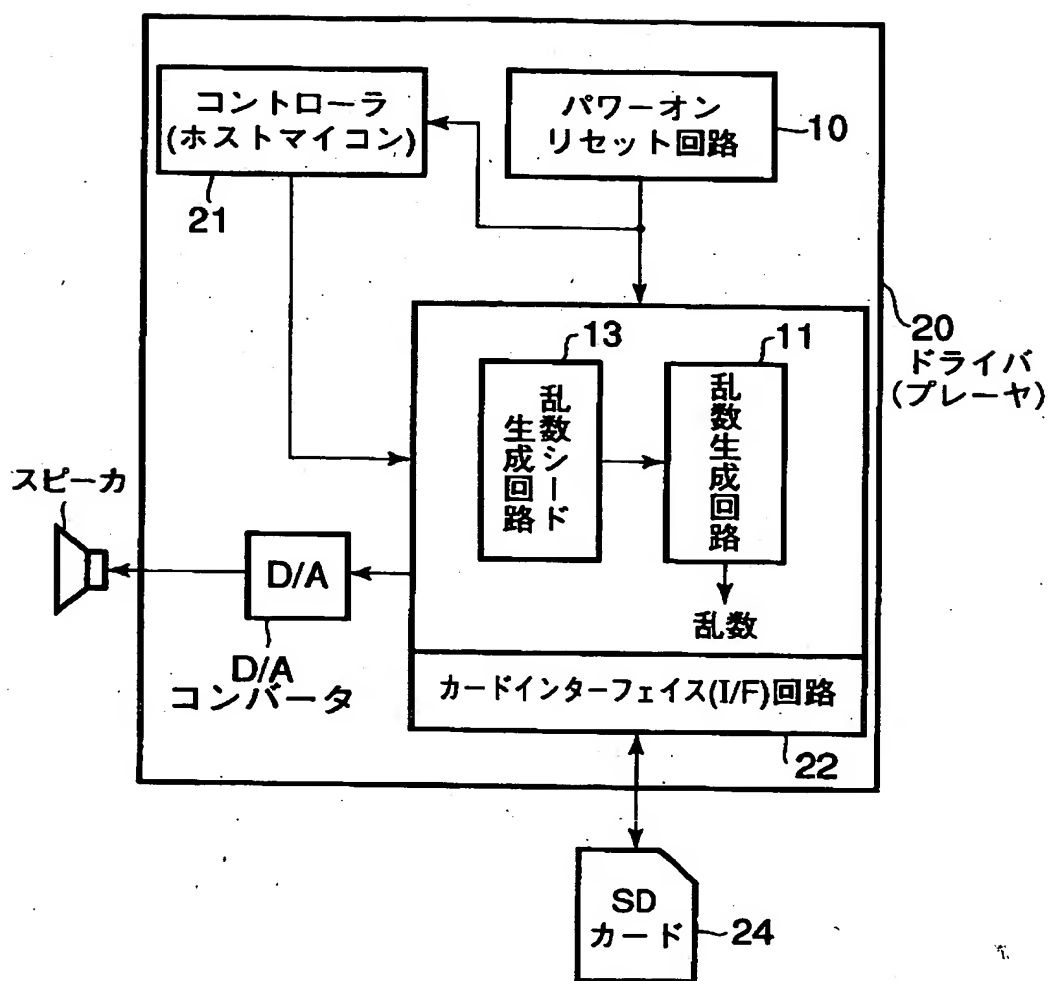
【図10】



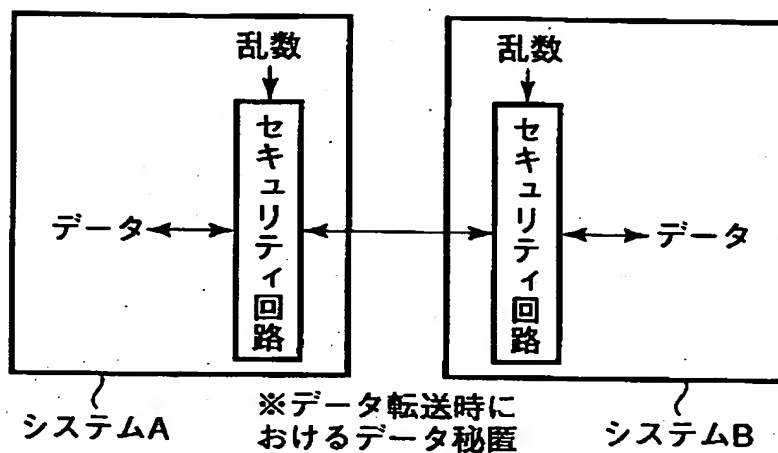
【図 11】



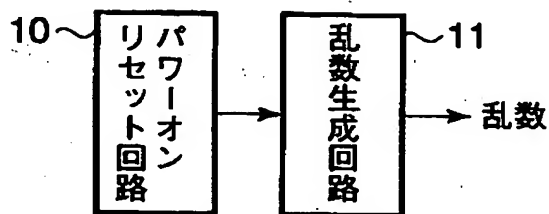
【図 12】



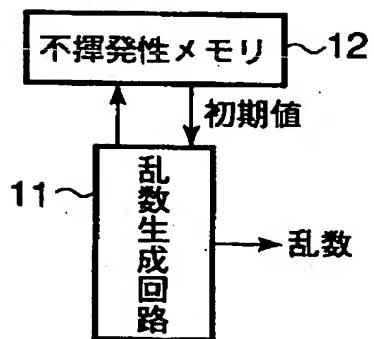
【図13】



【図14】



【図15】



【書類名】 要約書

【要約】

【課題】 不揮発性メモリなしに、起動の度に、乱数シードを変化させる。

【解決手段】 発振器 14 は、電源投入直後から動作し、高速クロックを発生する。カウンタ 15 は、この高速クロックにより動作し、カウント値を高速に変える。一方、電源が投入されてから十分な時間が経過した後、パワーオンリセット回路 10 は、内部電源が安定したことを示すパワーオンリセット信号を出力する。パワーオンリセット信号は、高速クロックよりも十分に遅く、また、ラッチ回路 16 に入力される時期も、まちまちとなるため、ラッチ回路 16 にラッチされるカウント値（乱数シード）は、電源が投入される度に異なるものとなる。この乱数シードを用いて、乱数が生成される。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日
[変更理由] 新規登録
住 所 神奈川県川崎市幸区堀川町72番地
氏 名 株式会社東芝
2. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝